



University of California HIPAA Education Module

Protected Health Information (PHI) Management Module for PHI Data Stewards

3/31/2003: Final

Copyright © University of California



Purpose

- This presentation has been prepared for all University workforce members who manage the use and disclosure of Protected Health Information (PHI). Your supervisor, HIPAA trainer or Privacy Officer should have also provided you with the *PHI Management Reference Manual (Reference Manual)*. The University's HIPAA Privacy Rule Education Modules and the *Reference Manual* should be used together to obtain information about HIPAA's requirements for releasing, accessing, handling health information and responding to requests from University patients about the use and disclosure of their information.
- The other UC HIPAA modules are: the UC HIPAA Provider Module, Research Module, Institutional Advancement and Media Module



Data Steward for PHI

Protected Health Information (PHI)

- Your job title or job description identifies you as a PHI Data Steward who:
 - Receives and reviews requests for PHI
 - Provides access to or releases PHI as permitted or required by HIPAA and other state or federal laws
 - Prevents access to or disclosure of PHI as permitted or required by HIPAA and other state or federal laws
 - Serves as the University's liaison to the patient, when the patient wants to exercise their Patient Rights provided by HIPAA or state law



Objectives

- Increase knowledge and understanding of HIPAA requirements and your important role as the Data Steward
- Identify risk areas and new policies
- Identify how California law and HIPAA provide patient rights and privacy protections



When do HIPAA rules apply to PHI and the work you do?

- Let me count the ways...
 - When you use it
 - When you disclose it
 - When you store or file it
 - When you see it on your computer
 - When it is lying on your desk
 - When you are talking about it face-to-face
 - When you are talking about it over the phone
 - When you transmit or store it electronically



HIPAA = Federal Law

- Establishes National Code Set Standards for electronic transactions and the transmittal of data electronically
- Provides for the privacy and security of an individual's health information
 - **Privacy Rule** (April 14, 2003) protects access to, uses and disclosures of an individual's protected health information (PHI) and requires security measures for that PHI.
 - **Security Rules** (April 20, 2005) requires physical and technical safeguards to protect the confidentiality, integrity and availability of PHI in electronic form
 - Potential civil and criminal penalties for non-compliance



Layers of Laws

- California law and JCAHO standards regarding patient privacy and confidentiality have existed for many years.
- Federal HIPAA Privacy Rule provides a national “floor” for providing patient rights and protection of PHI.
- California law pre-empts HIPAA when it provides greater patient rights or stronger protections for PHI



HIPAA Privacy Rule:

- **What information is protected?**
- **What is protected health information (PHI)?**



Protected Health Information (PHI)

- Health Information created or received by a health care provider, health plan, health care clearinghouse (“covered entity”) that relates to the past, present or future physical or mental health or condition of the individual, the provision of health care to the individual or the payment for the provision of health care and identifies the individual.
 - Including one or more of 18 identifiers and demographics
- Transmitted or maintained in any form or medium



What is NOT PHI?

- Employee Records
- Student Family Educational Rights & Privacy Act (FERPA) Records
- Research records that were not created as a result of providing health care services
- However, other state and federal laws require UC to protect the confidentiality of this health information

Permitted and Required Uses and Disclosures of PHI

- To the individual (required)
- To DHS to investigate compliance (required)
- For Treatment (T), Payment (P), Health Care Operations (O)
- Incidental to a use or disclosure that is permitted
- Authorized by the individual
- To Business Associates (permitted)
- When individual does not have the opportunity to object and Authorization not required
 - Public health activities, law, health oversight, judicial and administrative proceedings, etc.
- When covered entity (UC) provides an opportunity for Individual to Agree or Object
 - Facility Directory, or individuals involved in patient's care, or disaster relief
- Creation of Limited or De-identified Data Sets



Covered Entities Must Provide Notice of Privacy Practices (NPP) to Patient

- **University of California's NPP describes:**
 - Permitted & required uses / disclosures of PHI by CE
 - Patient's rights (and how to exercise the rights)
 - CE's legal duties with respect to PHI
- **Direct Treatment Providers must provide Notice**
 - No later than the date of first service delivery
 - Make a good-faith effort to obtain written Acknowledgement of receipt of the Notice (document)
 - Document reason Acknowledgement not obtained
 - Provide Notice as soon as reasonably possible in an emergency situation, but no Acknowledgement required
- **By Health Plans**
 - At compliance date and at enrollment of new enrollees
 - Every 3 years, must tell enrollees of Notice availability



MNS - Data Stewards Determine the Minimum Necessary

- Data stewards may reasonably rely upon the requestor's determination as to the minimum amount necessary, **IF** the request is from:
 - Another covered entity, e.g., hospital, provider, health plan with a relationship to the patient
 - Business associate for provision of professional services
 - Researcher with IRB Letter of Approval and Waiver of Authorization
 - Public health official
- Use professional judgment. If in doubt, refer non-routine requests to your supervisor or call the HIMS-Release of Information Unit



Minimum Necessary Standard (MNS)

- Use or disclose only the minimum PHI that you need to know to do your job
- Limit access, use or disclosure of PHI by others to the minimum amount necessary to accomplish the intended purpose
- A “think twice” standard:
 - Is it reasonable?
 - Is it necessary?



Uses and Exceptions to the Minimum Necessary Standard

- Disclosures to providers for treatment
- Disclosures to the patient
- Uses / disclosures with an authorization
- Uses / disclosures required for HIPAA standard transactions
- Uses / disclosures required by law
- Disclosures to HHS/OCR for enforcement



Categories of “Requestors”

- This section describes HIPAA’s requirements and your responsibility for responding to requests for access, use and disclosure of PHI
- There are 5 types of Requestors:
 1. Patient and Patient Representatives
 2. Provider Team & other members of the Workforce
 3. Third Party C.E.s for TPO (e.g., Other Hospitals)
 4. Researchers
 5. Third Party C.E.s – Non-TPO (e.g., Public Health)
 - *C.E. = Covered Entity*
 - *TPO = Treatment, Payment, Healthcare Operations*



#1. Requests from Patients or Patient Representatives

- Patients or patients representatives may request information from their Designated Records Set (DRS)
- A Designated Records Set is a group of records maintained by or for a Covered Entity (CE) that is:
 - The medical and billing records about individuals;
 - The enrollment, payment and claims adjudication records and case or medical management record systems maintained by or for a health plan; or
 - Information used in whole or in part by or for the CE to make decisions about individuals.



Requests from Patients or Patient Representatives

- All patient/patient representative requests should be in writing to the University
- Failure to follow HIPAA requirements for responding to patient/patient representative requests is a violation of HIPAA
- If you have questions, contact the Privacy Officer or a Supervisor



Personal Representatives of the Patient

- **The HIPAA definition of a “personal representative”** is someone who is authorized to act on behalf of an individual who is an adult or emancipated minor in making healthcare decisions, including signing an authorization for disclosure of PHI.
- **The scope of access depends upon the authority granted to the personal representative by state law.**
 - For purposes of inspecting and copying an individual’s PHI, a representative may include: a guardian or conservator; an executor or beneficiary or next of kin for a decedent; a parent or legal guardian of a unemancipated minor (unless the minor has that right); a person authorized to make health care decisions under a patient’s advanced health care directive.
 - Use professional judgment



Identifying the Personal Representative

■ Personal Rep – Minors

- Parent or guardian usually has the authority to make healthcare decisions about an unemancipated minor

■ Personal Rep – Deceased Patient

- Executor, Administrator or other person with authority to act on behalf of a deceased patient

■ Personal Rep – Adults and Emancipated Minors

- Conservator, Agent with Health Care Power of Attorney, or other person who has the authority to make healthcare decisions for an emancipated minor or adult who is unable or unwilling to make decisions

➤ Examples of Exceptions to authority to act:

- When a minor is a possible victim of violence, abuse or neglect
- When a minor can consent to the healthcare, e.g., reproductive and/or substance abuse counseling, sensitive services
- General power of attorney vs. Healthcare power of attorney: Scope of access varies!



What Can be Disclosed to a Personal Representative?

- Use professional judgment and experience to determine what PHI should be disclosed
- A patient's objections to disclosures should be honored
- Obtain a signed authorization for requests to access or obtain copies of PHI



Communication with Individuals Involved in the Patient's Care

- Exercise professional judgment & discretion
- Minimum necessary for disclosures of PHI to individuals involved in the patient's care
- Respect approved requests for confidentiality & restrictions
- Refer to the facility inpatient directory before releasing any inpatient information. There may be restrictions!



Considerations for Granting Access to PHI for Personal Representatives

- Verify the identity of the requestor and the authority to have access to PHI
- **Use professional judgment: You may deny access / copies of PHI for suspected abuse, neglect and endangerment situations or where access to PHI is reasonably likely to cause harm**
 - In this situation, the reason for denial will be determined by a healthcare provider or with consultation and approval from a HIMS Supervisor or Risk Management
- **Other exceptions may limit PHI disclosure to a specific care decision, e.g., a limited health care power of attorney for life support decision.**
 - This individual may not authorize PHI disclosures for unrelated purposes.



Billing Process

- Patients may request access to all payment / billing records “used to make a decision” regarding his/her benefit coverage, e.g., patient accounting notes or individual healthcare claim status notes; health plan eligibility notes.
- Determination of what parts of the claim record are **decision notes** must be made.
- Data stewards can provide a summary of the “decision notes”, if this is acceptable to the patient. UC may charge a reasonable fee for copies / postage
- **Tip: Only record relevant notes that are appropriate for viewing.** Be aware: Time frame for response



#2. Requests for PHI from UC Workforce Members and UC Business Associates Who are Covered by the Privacy Rule

Healthcare Provider Team,
Faculty Physicians and Health Professional Trainees,
UC Business Associates,
Workforce members who provide Business, Financial,
Legal Services to the CE
Volunteers and others under the direct control of the
University



HIPAA Permits Use and Disclosure of PHI for Treatment, Payment & Operations (TPO)

- **Treatment (T)** – The provision, coordination, or management of healthcare by one or more health care providers, including consultations and referrals
- **Payment (P)** – Activities to obtain payment or be reimbursed for health care services; health plans to obtain premiums, fulfill coverage responsibilities, or provide reimbursement
- **Health Care Operations (O)** -- Administrative, financial, legal and quality improvement activities; business planning activities; training, teaching; accreditation, credentialing, licensing, competence, performance activities; fraud, abuse, compliance activities

The University's Notice of Privacy Practices describes the specific uses and disclosures of TPO



Disclosure of PHI for Payment Activities

- PHI can be disclosed to workforce members and Business Associates involved in obtaining payment for UC healthcare services (MNS applies)
 - Business Associates (outside contractors or vendors) must sign a Business Associate Agreement with UC in order to access, use or disclose PHI on UC's behalf
 - Coding and billing staff, utilization review, third party payers, financial transactions
 - Transmit the data in a secure, confidential manner (see policy on e-mail transmission)
- MNS applies to access, use or disclosure for payment activities



Requests for Billing Data received by Phone

- For phone requests, when the caller is the financial guarantor or other third-party payer, you may disclose by phone the minimum billing PHI for the episode of care to facilitate payment.
- Considerations:
 - Use professional judgment and discretion
 - Verify identity of caller, e.g., what is the account #, or last 4-digits of beneficiary's SS#, or other identifier?
 - Provide minimum necessary PHI for the specific episode of care in question; document the release of PHI in the claim notes
 - Be aware of any approved 'alternative communications', e.g., alternate address or phone #



Requests for Written Documentation in Support of a Medical Claim / Billing


- Requests from payers: MNS for the episode of care (e.g., specific claim in question)
 - Transmit the material in a secure manner
 - Use fax cover sheets (verify fax #/addresses) or
 - Use sealed envelope with a cover letter
 - Do not use unsecured E-mail
- Requests from patient or a guarantor for copies of PHI for the medical billing claim (medical records, claim records):
 - Patient (or legal representative) authorization is required for any release of information
 - Use the UC_ Authorization Form
 - Forward the request to the appropriate data steward, e.g., HIMS



Use and Disclosure of PHI for Health Care Operations (O)

- Fundraising, Community and Media Relations
- Training of health care professionals is a part of operations (MNS applies)
 - UC teaching activities within UC, with UC teaching affiliates and with other teaching institutions
 - Training of health professionals from other CEs who are UC teaching affiliates
- Quality/Peer Review Activities
- Business Planning and Development

For all operations, MNS applies. For some uses and disclosures, there are further restrictions. See PHI Reference Manual.



Uses and Disclosures of PHI for Fundraising by Staff and Faculty

- UC may only use demographic information and dates of service to create fundraising lists, fundraising databases and send out fundraising materials to patients
 - Disease, diagnosis or condition may not be used to develop a fundraising mailing list. An existing data base may not be used except with a patient's Authorization that meets all HIPAA requirements for a valid Authorization
- Faculty may provide the Development Office with a list of individuals and contact information for specific fundraising appeals
 - For example, Development Office may request that all faculty provide a list of names for a fundraising event for the Cancer Center
- All fundraising material must provide the recipient with a way to opt out of receiving future fundraising materials
- All fundraising efforts must be coordinated with the UC_HS or campus Development Office.



Use & Disclosure of PHI to UC Faculty and Health Care Trainees

- Use and disclosure of PHI for the teaching of all UC health professions programs students are part of health care operations (MNS always applies & students must be HIPAA trained—see Provider Module)
- When non-UC health care trainees are participating in a UC training program (e.g., students from affiliated teaching institutions that are also CEs), they are a part of the UC workforce and must be HIPAA-trained
 - However, trainees from UC affiliated institutions must have a teaching relationship to the patient in order to use PHI for teaching purposes at the sponsoring affiliated institutions
- Trainees, who are also providing healthcare to the patient, may have access to the patient's complete PHI, if necessary.



Requests from Trainees for PHI/Medical Record

- Data Steward must determine purpose for access / use / disclosure of PHI—does the trainee have a teaching or treatment relationship to the patient?
- MNS always applies for teaching and health care operations
- Determine whether the requestor is a UC trainee or a trainee from a UC affiliate
- If access is for research by the trainee, other rules apply
- If Trainee is NOT from an affiliated CE (e.g., another academic medical center or hospital), then the Trainee may only disclose to his/her sponsoring institution data contained in the following:
 - Limited Data Set with a Data Use Agreement with sponsoring institution, or
 - De-Identified data

Remind trainee: No re-disclosure or re-identification of PHI data is permitted; shred when finished.



Be Aware:

- **HIPAA does not allow UC Faculty or trainees to disclose PHI to individuals who do not have a teaching relationship to UC or a teaching relationship to the patient**
 - Example: Individuals at CME conferences or medical/health lectures
- **Disclosure of PHI in these circumstances is limited to:**
 - De-identified data; or
 - Limited Data Set and Data Use Agreement; or
 - Patient's written authorization
 - As members of the UC Workforce, faculty and trainees may create the Limited or De-identified Data Set using the medical record.
- Seek help from the Privacy Official or a Supervisor if questions arise.



UC Business Associates

- Business Associates are third-party vendors or contractors who use or disclose PHI on behalf of the UC covered health care providers and health plans for TPO and other activities
 - UC must identify all Business Associate relationships
 - Examples: External billing agencies, third party administrators, outside counsel, accreditation agencies
 - See PHI Reference Manual for specifics
- Business Associate Agreement required that provides assurances Business Associates will protect PHI
- If an individual or entity requests PHI and claims to be a Business Associate, verify with Privacy Officer or Procurement / Purchasing Manager
- Document and retain all signed Agreements

#3. Requests for PHI from Third Parties for TPO



Other Covered Entities — for Treatment, Payment, Operations, including training of health care professionals



Disclosure of PHI to Other CEs

- **Treatment (T):** The CE may provide PHI for ongoing treatment by another healthcare provider, health plan or non-covered healthcare provider or entity
 - No Business Associate agreement is required
 - No MNS required
- **For Payment (P):** The CE may receive or disclose PHI for payment purposes of a covered or non-covered health care provider or covered health plan
 - No Business Associate Agreement is required
 - MNS applies and there must be a relationship to patient



Disclosure of PHI to Other CEs

- **For Operations (O):** The CE may disclose PHI only to another CE or its Business Associates for the following:
 - Quality assessment and improvement; population-based activities to improve health or reduce health care costs, case management, certification, accreditation, licensing, credentialing, conducting training, health care fraud and abuse detection and compliance
 - MNS applies and there must be a relationship to the patient
 - For all other O, CE must provide either a LDS with Data Use Agreement, DDS or obtain patient Authorization for disclosures of PHI
- **For Research Purposes** of another CE, Research is not O
 - UC Institutional Research Board (IRB) policy requires the participation of a UC investigator on any research conducted by an outside researcher with UC patients or patient records



Tracking Disclosures to Other Covered Entities (C.E.s)

- The CE must track all disclosures to other CEs except those disclosures:
 - For TPO (Business Associate relationships to carry out TPO do not require tracking if a Business Associate Agreement is in place)
 - Authorized by the Patient
 - Provided with a LDS/Data Use Agreement or DDS

See PHI Reference Manual for detailed list of required tracking of disclosures



#4. Use and Disclosure of PHI to University Researchers

Research is not a covered function under the HIPAA Privacy Rule, but research confidentiality is protected under the Common Rule. Researchers want access to the CE's PHI for research purposes. HIPAA requires the CE to be assured that PHI disclosed for research activities will be protected. This is the role of the UC Institutional Review Boards (IRBs). The IRBs review all protocols requiring PHI and provide assurance to the CE.



Use & Disclosure of PHI for Research

- Researchers, including Faculty Physicians, must provide the CE with an IRB Letter of Protocol Approval and one of the following prior to receiving PHI for research purposes
 - 1. Patient's / Subject's Authorization**
 - See UC Authorization for Research
 - Authorization may be combined with Informed Consent
 - Specific requirements for ongoing research approved prior to April 14, 2003
 - 2. IRB Waiver of Authorization**
 - 3. Request for a Limited Data Set or a De-identified Data Set**
 - UC researcher may act as member of the workforce to create the LDS, if HIPAA trained and signed Confidentiality Agreement.
 - Use of a LDS requires a Data Use Agreement



Documentation Requirements

IRB Study # and signed Letter of Approval	Retain copies of all IRB Letters of Approval
Patient Authorization	Retain a copy of the valid, signed authorization
IRB Waiver of Authorization	Retain a copy
Limited Data Set (LDS)	Retain a copy of signed Data Use Agreement
De-Identified Data Set (DDS)	Document if researcher created DDS



#5. Disclosures to Third Parties for non-TPO Activities

Permitted or Required Reporting, such as.,

Public Health

Food & Drug Administration (FDA)

Authorized Agency for Required Reporting

Health Oversight Activities

Others: Court Requests; Law Enforcement; Coroners...

Permitted or Required Disclosures for Public Health Activities

- To a public health authority authorized by law to receive PHI to prevent or control disease, injury or disability
- To the FDA for activities related to the quality, safety or effectiveness of an FDA-regulated product or activity, including adverse event reporting
- To an authorized agency for reporting of victims of abuse or neglect (see distinction for children vs adults)
- For health oversight activities
- To an employer regarding a member of the workforce for workplace medical surveillance or a work-related illness or injury
- All other disclosures to the employer require the employee's Authorization



Other disclosures

- To a court or administrative tribunal for judicial and administrative proceedings
- To law enforcement individuals for law enforcement purposes; or for reporting crime in emergencies
- To coroners and medical examiners for identifying a deceased person and to funeral directors
- To Organ Procurement Organizations to facilitate donation and transplantation

Verify identity of the requestor, legal authority for the request and the purpose for the request. Minimum necessary standard applies

There are specific requirements that must be met, including some State law that is more stringent, and documentation and accounting requirements.

See the PHI Reference Manual.



Self-Test

- **May the PHI Data Steward release PHI when...**
 - Researcher requests access to PHI of diabetic patients admitted to the hospital.
 - *Answer: No, unless the PHI has been de-identified, is disclosed in a limited data set or has patient authorization.*
 - Clinician requests access to a colleague or spouse's PHI. (He/she is NOT a member of the treatment team.)
 - Non-UC pharmacy reps request a list of patients on a treatment regimen for marketing purposes.
- *Answer: No, unless the patient or patient's representative has provided written authorization.*



Special Provisions for PHI From Which Some or All Patient Identifiers Have Been Removed

- De-identified Data Set (DDS)
- Limited Data Set (LDS)
 - Data Use Agreement



De-identified Data Sets (DDS)

- **HIPAA allows the CE to create, use or disclose a De-identified Data Set**
 - No Patient Authorization required
 - No tracking of disclosures
 - Researchers may act as members of the workforce to create a de-identified Data Set if they have received HIPAA training.
- **CE must De-identify the Data Set by 1 of 2 methods:**
 - Application of a statistical method that renders information not individually identifiable; or
 - Stripping of 18 listed identifiers for patients, relatives, employers, or household members, such as:
 - Names; geographic subdivision (city, state, zip Code);
 - All elements of dates (date of birth, death, service)
 - Social Security numbers, medical record numbers, patient account numbers, etc.



Limited Data Sets (LDS)

- **HIPAA allows the CE to create, use or disclose a LDS for research, public health disclosures and health care operations**
 - No Patient Authorization required
 - No accounting of Uses and Disclosures with LDS
 - Recipient of the LDS must sign a Data Use Agreement (see UC Boilerplate)
 - UC should retain Data Use Agreements
 - Researchers may act as members of the workforce to create a LDS, if they have received HIPAA training and have signed a Confidentiality Agreement
- **LDS removes direct identifiers of the individual, relatives, employers or household members, but allows ... age, dates, ethnicity and zip code**
 - Dates of admission, discharge and service, date of birth / death



Use of Limited Data Sets (LDS)

- HIPAA allows the use of a limited data set for certain purposes: HCO, teaching, research, and public health reporting
- Examples of when to use LDS for requests for PHI:
 - Allied health professionals at a non-University of California school
 - CME and other education to individuals who are not part of UC
 - Teaching materials for undergraduate education
 - Research purposes



Authorizations

for Access, Use/Disclosure of PHI

Authorization Form Requirements:

See UC Authorization Form

■ Elements

- Description of PHI and purpose of disclosure
- Name of person(s) or class of persons authorized to disclose PHI
- Name of person(s) or class of persons authorized to receive PHI
- Expiration date / event
- Signature of patient (or personal rep.) and date
- If personal rep signs, state relationship to patient

■ Required Statements:

- Right to refuse to sign and Right to revoke
- CE may not condition treatment, payment, enrollment or eligibility for benefits
- Potential for re-disclosure of disclosed information

■ Other requirements:

- Plain language
- Copy to the individual
- Retain for 6 years
- Disclosure of remuneration (if applicable)



Examples of Disclosures Requiring an Authorization

- Release of PHI to an individual's lawyer
- Release of a list of patients to a drug company or other third party
- Release of PHI to the patient's employer
- Release of PHI to the media or for PR purposes
- Release of PHI to a researcher for an IRB Approved protocol that requires Authorization
- Creation of fundraising lists using patient diagnosis or treatment
- Release of Psychotherapy Notes



Patient's Privacy Rights

1. To receive a copy of the “**Notice** of Privacy Practices” (NPP)
2. To request alternative **confidential communications**
3. To request **access** to and copies of PHI in the DRS
4. To request an **amendment** / addendum to the DRS
5. To request an **accounting** of disclosures of PHI
6. To request **restrictions** or limitations on use / disclosure of PHI
7. Opportunity to agree or **object**—opt out of the facility directory; disclosures to family, friends; receive fundraising materials
8. To file a **complaint** about privacy practices

The University must respond when patients wish to exercise these rights. See NPP (Notice) and PHI Reference Manual.



Patients must have an Opportunity to:

- Opt out of the Facility Directory (inpatient)
- Object to uses and disclosures ...
 - To family members or friends or patient advocate
 - In the Facility Directory
- Request alternative forms of Confidential Communications
- Request restrictions on uses and disclosures:
 - For Treatment, Payment and Operations
 - To individuals involved in patient's care
- Designate a personal representative
- To opt out of fundraising and marketing

Refer non-routine requests to the Privacy Official or Risk Manager for review.



Facility Directory (Inpatient)

Patient information - What may be disclosed

- Facility Directory Information: name, location, general condition; and for clergy, the religious affiliation
- Facility Directory Information may be provided to persons who request the individual by name (including media), unless:
 - Patients restricts or prohibits use or disclosure, e.g. no phone calls, no visitors, no clergy, no disclosure
 - In emergency, CE's professional judgment to designate the admission as "no disclosure", e.g., patient safety
- Disclosures to clergy permitted, unless patient requested "no disclosure":
 - "No Disclosure" means no disclosures may be made, e.g., "I have no information on this patient."
 - Patient request may be written or oral and may be made at any time.



Patient's Request for Confidential Communications

- Patients may request alternative means of receiving communications of their PHI
- All requests, denials of requests and approvals should be in writing
- All reasonable requests must be permitted and accommodated
- The requirement applies to disclosures by health plans if the individual clearly states disclosure could endanger individual
- UC data stewards will determine if the request is reasonable and will **document** all approved requests
- **Examples of reasonable requests:**
 - Send bills to a P.O. Box, rather than a home address.
 - Route follow-up calls to a cell-phone number, rather than home #.
 - E-Mail: Obtain patient's authorization prior to sending, exercise caution



Patient's Request for Access to and Copies of PHI in the DRS

- Patient has a right to request access to inspect and/or obtain a copy of his/her PHI in a DRS for as long as the DRS is maintained
- All requests for access and any denials must be in writing
- Timely response is required
- UC may charge a reasonable cost-based fee for copying and mailing and for preparing an executive summary if patient requests a summary
- HIPAA provides specific requirements for denial of access in very limited circumstances and provides a right to an appeal of the denial
- Refer to the PHI Reference Manual and local campus policies for guidance



Patient's Request to Amend the Designated Record Set

- A patient has the right to request the CE to amend PHI in the DRS
- All requests should be in writing
- HIPAA provides specific criteria for denying a request and providing a timely, written response to the request UC providers may deny the request for an amendment
- Patient has right to disagree with the denial and provide a rebuttal
- California Law permits a patient to submit an addendum to the medical record (up to 250 words per incorrect item). UC cannot refuse the request to include an addendum.
- See the PHI Reference Manual for detailed instructions



Patient's Requests for an Accounting of Disclosures of PHI

- Patients have the right to receive an accounting of disclosures of PHI made by a CE in the 6 years (or less) prior to the date of the request
- No accounting is required for disclosures prior to April 14, 2003 or disclosures for:
 - Treatment, Payment, Operations (including Business Associates)
 - Limited or De-identified Data Sets
 - Authorized or Incidental Disclosures
- Accounting requirement applies to disclosures where the patient has not had an opportunity to agree or object and pursuant to research Waiver of Authorizations (see PHI Reference Manual)
- UC must respond in writing and in a timely manner
- First accounting in a 12-month period is free; charge for subsequent requests



Accounting for Disclosures

What must be documented?

- Name of who received the PHI and address (if known)
- Description of the PHI that was disclosed
- Date of disclosure
- Purpose of the disclosure, e.g., required public health reporting, FDA, law enforcement request, subpoena, ...
- Refer to the PHI Reference Manual and UC_HS policy for the list of routine disclosures that must be documented, and the procedure for reporting disclosures, e.g., disclosure form, or an on-line reporting system



Patient's Requests for Restrictions

- UC must permit an individual to request restrictions on the uses and disclosures of PHI for TPO purposes and for disclosures to persons involved in an individual's care
- Requests should be in writing
- BUT ...UC is not required to agree to such requests, nor provide review or appeal
- If UC agrees, then UC may not violate the restriction except in cases of emergency
- Consideration may be given for requests to restrict disclosures where there may be social stigma, celebrity status and/or risk of potential violence to the patient.
- Refer requests to the UC_HS Privacy Officer or Risk Manager.



Patient's Right to File Complaints

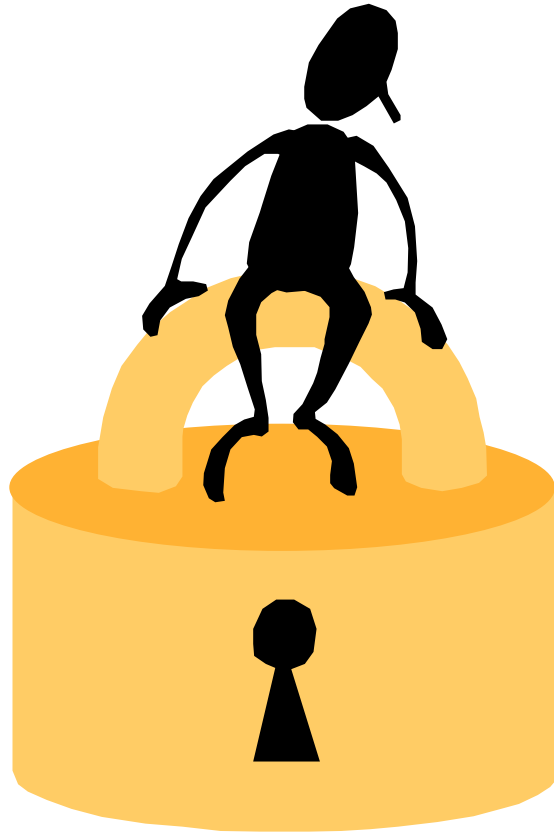
- Patients have the right to complain to UC about violations of their privacy / security and/or to the Department of Health & Human Services (DHHS)
- The NPP advises patients and others where they can file a complaint
- Respond to complaints and document any action taken
- The NPP is also posted on the UC_HS website at:
<http://>
- Action: Refer to PHI Reference Manual for policy / procedures for complaints.

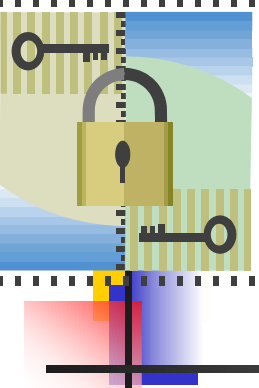


Self-Test

- Do you know what to do when a patient requests those Rights provided under HIPAA?
- Do you know where to get help?
- Do you know when the Minimum Necessary Standard applies?
- Why is your role as PHI data steward and gatekeeper of the DRS so important?

HIPAA also requires Security





It's Good to Know: Privacy & Security Go Hand-in-Hand

- **Privacy focus is – “Who can access, use or disclose information?”**
 - “What is Private?” is a key concept
 - Patient’s rights to know how information is used and disclosed
 - Patient’s right to control access to information
- **Security focus is – “How do we keep it private?”**
 - Privacy Rule - protects security of information in all forms
 - Security Rule - protects electronic information



HIPAA – Security Tips

- Security of electronic data: **Your responsibility!**
 - Password security is key...NEVER SHARE PASSWORDS
 - Password protect your PCs, PDAs, laptops, home computers; use automatic log-offs
 - Secure access, transmission, storage and retention of e-data
 - Don't leave confidential information on your computer screen...or in the trash! Do not e-mail PHI outside the network unless you can encrypt it
 - Use caution when sending faxes. Be aware of who may be viewing the information from both fax machines. Use fax cover sheets and verify fax #s.
 - Report breaches to your UC privacy / security officer.
- Physical security of data: **Your responsibility!**
 - Use locked shredder bins; Key access to file rooms / cabinets



Self-Test: Security

Question: For new hires & temporary personnel, when can I share my password to avoid delaying patient care and/or billing?

Choices: *(choose the 1 correct answer)*

- A. I may share my password with new personnel for up to 10 days or until the person has their own password, as long as they have completed privacy training.
- B. I may post my password in a discreet area to limit access to my password.
- C. Only when temporary personnel are hired or students are visiting.
- D. Never!

▪ *Answer: "D"*



Summary

- To build trust with our patients, the HIPAA Privacy Rules call on all of us to learn and implement the privacy and security rules regarding protected health information (PHI)
- ...and abide by them!

Understand and Use New UC Policies for HIPAA Privacy Rule

- **Access, Use and disclosure of PHI** for TPO, teaching, fundraising, research and the Minimum Necessary Standard
 - Respond to requests from patients to exercise their **Privacy Rights**
 - Set up systems to:
 - ✓ Track those disclosures that require an accounting
 - ✓ Document and retain required documentation for 6 years
 - **Updated policies for release of PHI** to personal representatives (adults, minors, decedents); and to law enforcement and governmental agencies
- **New / Updated Forms:**
 - “Notice of Privacy Practices” (NPP)
 - “Acknowledgement of NPP”
 - Authorization Forms
 - “Business Associate Agreements” (BAA)
 - Workforce “Confidentiality Agreement”

HIPAA

References and Resources

- UC_HS “Notice of Privacy Practices”
- UC Privacy Officer and UC_HS Privacy Officer for your campus
- UC HIPAA web site:
 - http://_____
- UC privacy / security / confidentiality policies
- HIPAA PHI Reference Manual is available at _____ to provide more detailed information on your local policies and procedures
- HHS Office of Civil Rights, HIPAA regulations
 - <http://www.hhs.gov/ocr/hipaa>



Document your Training

- If viewing this self-study module online, print out the training certificate form for your supervisor as proof of completing the module.



Training Certificate

Congratulations!

- You have now completed the “HIPAA PHI Management Module for PHI Data Stewards”.
- Disclaimer: This module is intended to provide educational information and is not legal advice. If you have questions regarding the privacy / security laws and implementation procedures at your facility, please contact your supervisor or the healthcare privacy officer at your facility for more information.

Print Name: _____ Dept.: _____

Signature: _____ Date: _____